In the Claims:

Please cancel claims 6 and 13-19. The claims are as follows:

1. (Previously presented) A method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

verifying by the browser the SCAC certificate using a new public key of the certifying authority.

2. (Previously presented) The method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

verifying the request by the certifying authority using the server's public key; and

generating the SCAC certificate by the certifying authority using a new private key of the

certifying authority and forwarding the SCAC certificate to the server.

3. (Previously presented) The method of claim 2 wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

4. (Previously presented) The method of claim 1, further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

5. (Previously presented) The method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake.

6. (Canceled)

7-10. (Canceled)

11. (Previously presented) The method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate.

12. (Previously presented) The method of claim 1, wherein obtaining the SCAC certificate

09/626,637   . 3

comprises using the new private key of the certifying authority.

13-19. (Canceled)